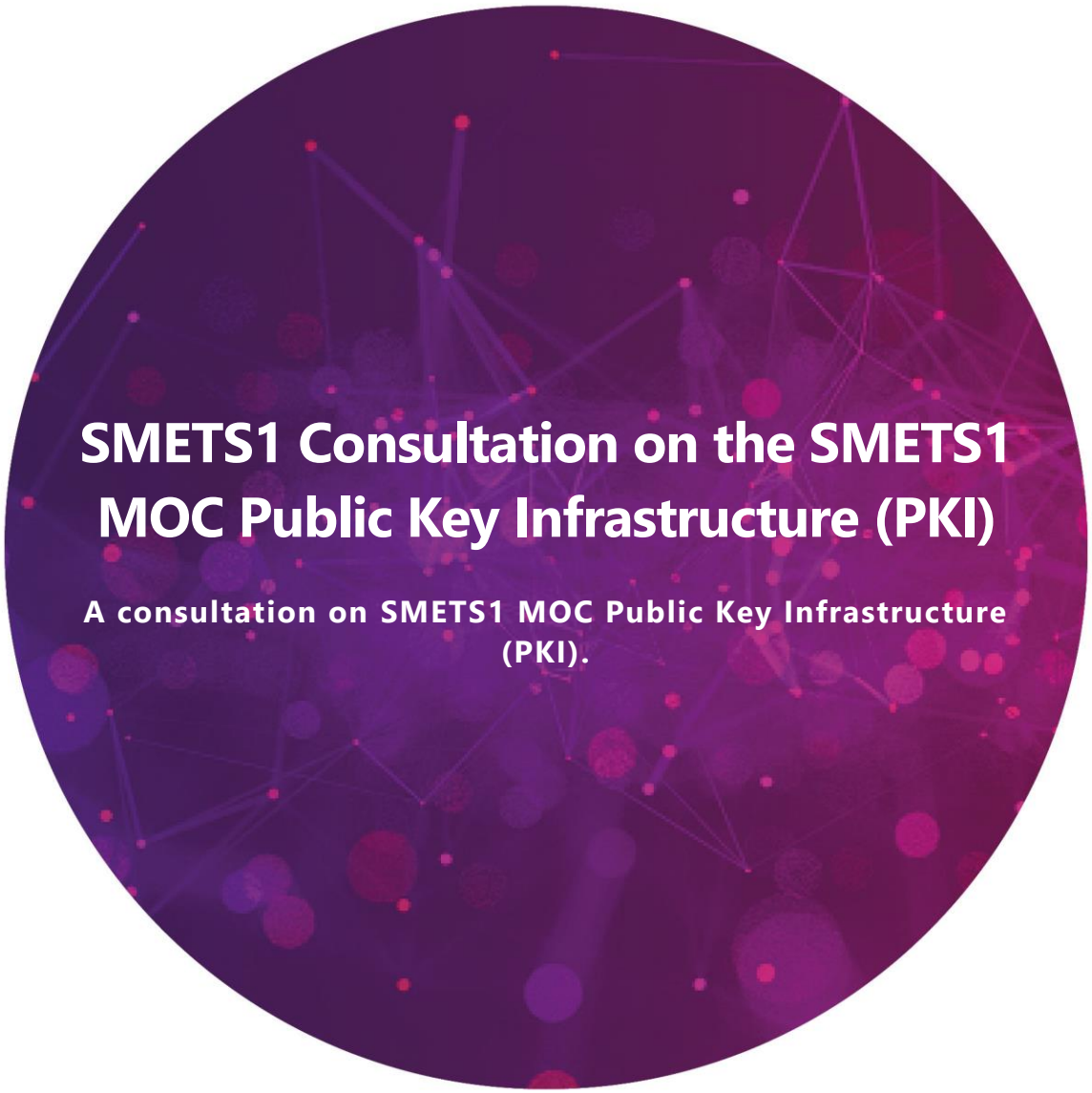
Data Communications Company



SMETS1 Consultation on the SMETS1 MOC Public Key Infrastructure (PKI)

A consultation on SMETS1 MOC Public Key Infrastructure (PKI).

Date: 17 July 2020
Respond by: 1600 on Friday 14 August 2020
Author: consultations@smartdcc.co.uk
Classification: DCC Public

Table of Contents

1. Introduction and Context 3
2. S1SPKM Compliance Policy and MOC Secure S1SP Certificate Policy 3
   - 2.1. S1SPKM Compliance Policy 4
   - 2.2. Secure S1SPKI Certificate Policy 4
3. Next Steps 4
4. How to Respond 5
5. Attachments 5
   - Attachment 1 6

1. Introduction and Context

In the initial stages of the smart meter roll-out across Great Britain, a number of energy suppliers installed first generation smart devices (known as SMETS1 devices), in consumers' premises. SMETS1 devices installed by one energy supplier, however, are not always interoperable with and supported by the systems used by another supplier. The Data Communications Company (DCC) has developed a plan and designed a solution for the incorporation of such devices into its national network. It provides important shared benefits for industry and consumers and intends to offer the ability for SMETS1 consumers to maintain their smart services following a decision to switch suppliers.

SEC Section L of the SEC sets out the arrangements that govern the Smart Metering Key Infrastructure (SMKI) which underpins the security of smart-meter related communications. In order to provide governance of the SMKI documentation and gain assurance of the DCC operation of the SMKI Services, the SMKI Policy Management Authority (SMKI PMA) was established under the SEC and serves as a Sub-Committee of the SEC Panel.

Depending on the SMETS1 Service Provider (S1SP), communications to SMETS1 devices from S1SPs are secured using either a dedicated, non SMKI PKI or by using symmetric keys. BEIS introduced changes that aligned the management of these S1SP PKIs and the symmetric keys under the aegis of the SMKI Policy Management Authority (SMKI PMA) and required the incorporation of relevant documentation into the SEC. This was to ensure a consistent set of oversight arrangements on the management of keys that are used as part of the secure end-to-end communication for SMETS1.

In this consultation DCC seeking views on a proposed SMETS1 Service Provider Key Management (S1SPKM) Compliance Policy and S1SP Certification Policy for MOC Secure.

2. S1SPKM Compliance Policy and MOC Secure S1SP Certificate Policy

For the Secure S1SP, DCC is proposing to use a separate PKI to the existing version in the SEC for secure communication between devices and the MOC S1SP and DCO. As the PKI is an essential element of the end-to-end security of communications with their associated SMETS1 devices, BEIS placed this under the oversight of the SMKI PMA to provide a consistent set of oversight arrangements with SMKI. The result is that the certificate policies for the MOC PKI would, on incorporation into the SEC, need to be reviewed by the SMKI PMA in the same way that applies to the SMKI documentation. In practice both the Certificate Policy for Secure and the S1SPKI Compliance Policy have already been reviewed and approved by the SMKI PMA.

Section L provides that the SMETS1 PKI should be assured in the same way that the SMKI PKIs and IKI are assured. As a result, DCC is providing for consideration an equivalent of the SMKI compliance policy that applies to the additional SMETS1 MOC PKI (although this has been drafted in a generic manner to apply to all S1SPKIs). The SMETS1 PKI for MOC Secure suite of documents which DCC is seeking views on are, the S1SPKM Compliance Policy, and the MOC, Secure S1SPKI Certificate Policy . Further details of these documents are set out under the headings below.

2.1. S1SPKM Compliance Policy

Pursuant to Section L15 of the SEC, DCC is required to produce an S1SPKM Compliance Policy. The S1SPKM Compliance Policy is required to set out the manner in which DCC will facilitate an assessment of the DCC's compliance with any applicable requirements of the S1SPKM Document Set. The S1SPKM Compliance policy will further set out how the SKMI PMA shall exercise the functions allocated to it as well as how DCC shall procure all such services as are required for the purposes of complying with its obligations under the S1SPKM Compliance Policy.

The S1SPKM Compliance Policy has been written as a generic compliance policy to apply to all S1SPKIs rather than specifically the Secure PKI, although it will be kept under review as the S1SPKM Document Set is further populated.

PKI Q1	Do you have any comments on the S1SPKM Compliance Policy?

2.2. Secure S1SPKI Certificate Policy

Pursuant to Section L14.5 of the SEC, DCC is required to produces an S1SPKI Certificate Policy.

This Policy sets out the arrangements relating to:

- SS1SP End Entity Certificates; and
- SS1SPCA Certificates.

PKI Q2	Do you have any comments on the S1SPKI Certificate Policy for Secure?

3. Next Steps

Following the closure of this consultation, DCC will take into account respondents' views, and, subject to the consultation responses received, submit to the Department of Business, Energy and Industrial Strategy (BEIS) a version of the PKI documents that it considers suitable for designation into the SEC by the Secretary of State.

DCC is aiming to providing a report to BEIS by 4 September 2020. DCC has discussed the re-designation of the PKI documents with BEIS and it is proposed that, subject to timely receipt of DCC's report and copies of relevant stakeholder responses to this consultation, BEIS will designate the PKI on 11 September 2020 or as soon as reasonably practicable within one month thereafter.

In order to expedite the designation of the S1SR, DCC is also seeking views on behalf of BEIS on the proposed date for designation of the PKI documents as well as the draft direction which is presented in Attachment 1 of this consultation document for stakeholder consideration.

PKI Q3	Do you agree with the proposed designation date of 11 September 2020, or as soon as reasonably practicable within 1 month thereafter for both the SISPKI Compliance Policy and Certificate Policy for Secure?

4. How to Respond

Please provide responses by 1600 on 14 August 2020 to DCC at consultations@smartdcc.co.uk.

Consultation responses may be published on our website www.smartdcc.co.uk. Please state clearly in writing whether you want all or any part, of your consultation to be treated as confidential. It would be helpful if you could explain to us why you regard the information you have provided as confidential. Please note that responses in their entirety (including any text marked confidential) may be made available to the Department of Business, Energy and Industrial Strategy (BEIS) and the Gas and Electricity Markets Authority (the Authority). Information provided to BEIS or the Authority, including personal information, may be subject to publication or disclosure in accordance with the access to information legislation (primarily the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004). If BEIS or the Authority receive a request for disclosure of the information we/they will take full account of your explanation (to the extent provided to them), but we/they cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded by us as a confidentiality request.

If you have any questions about the consultation documents, please contact DCC via consultations@smartdcc.co.uk.

5. Attachments

- Attachment 1 – Draft designation
- Attachment 2 – S1SPKM Compliance Policy
- Attachment 3 – S1SPKI Certificate Policy for Secure

Attachment 1

This attachment contains the text that BEIS plans to use for direction of changes to the S1SR.

PKI for Secure Draft Direction Text

This direction is made for the purposes of the smart meter communication licences granted under the Electricity Act 1989 and the Gas Act 1986 (such licences being the "DCC Licence") and the Smart Energy Code designated by the Secretary of State pursuant to the DCC Licence (such code being the "SEC").

Words and expressions used in this direction shall be interpreted in accordance with Section A (Definitions and Interpretation) of the SEC.

Pursuant to Condition 22 of the DCC Licence and Section X5 (Incorporation of Certain Documents into this Code) of the SEC, the Secretary of State directs that, with effect from [DD MMM YYYY], the S1SPKI Certificate Policy for Secure and the SISPKI Compliance Policy will be designated and incorporated into the SEC as Appendix XX and Appendix XY respectively in the form set out in Annex [XX] and Annex [XY] respectively to this direction.

This direction is also being notified to the SEC Administrator.